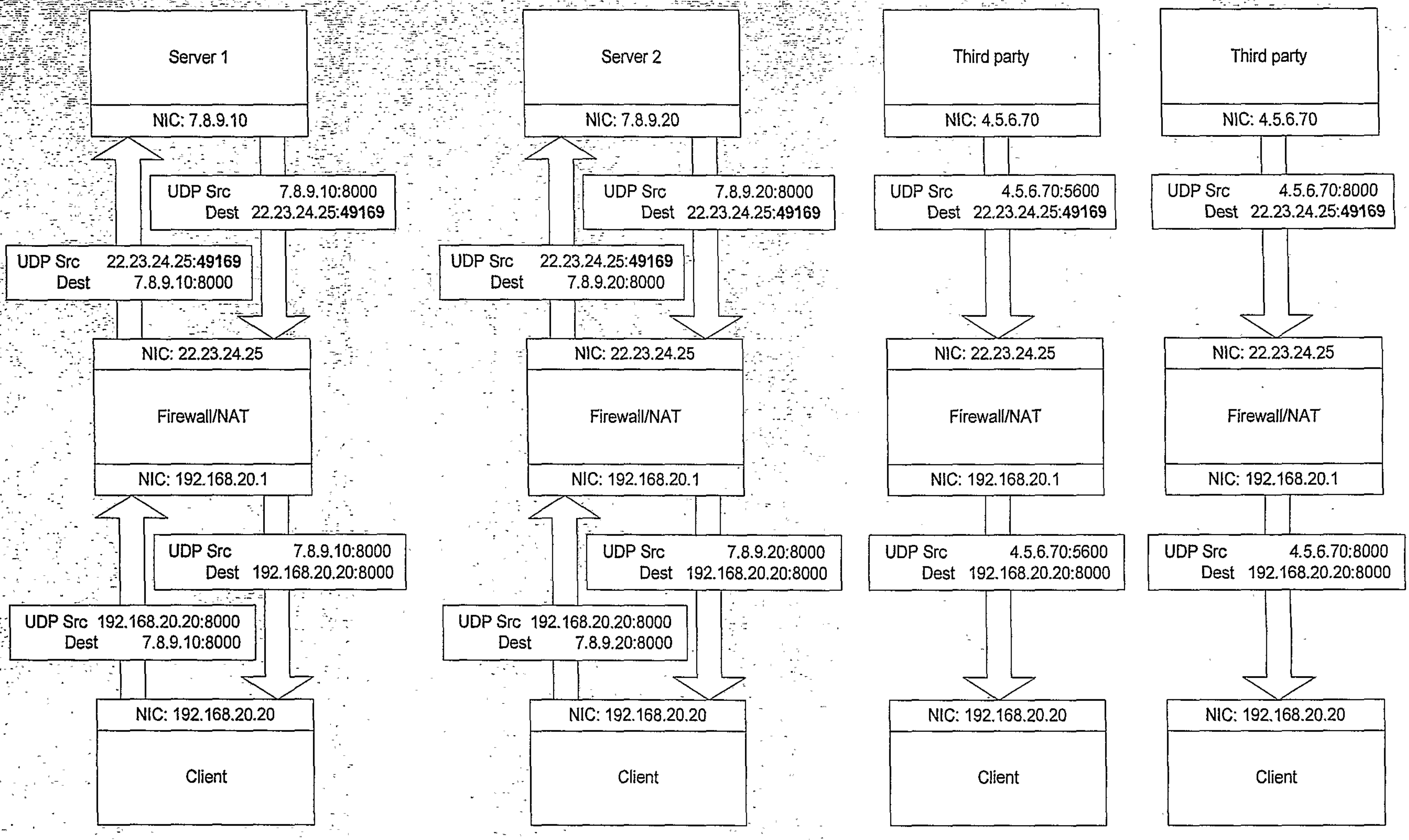


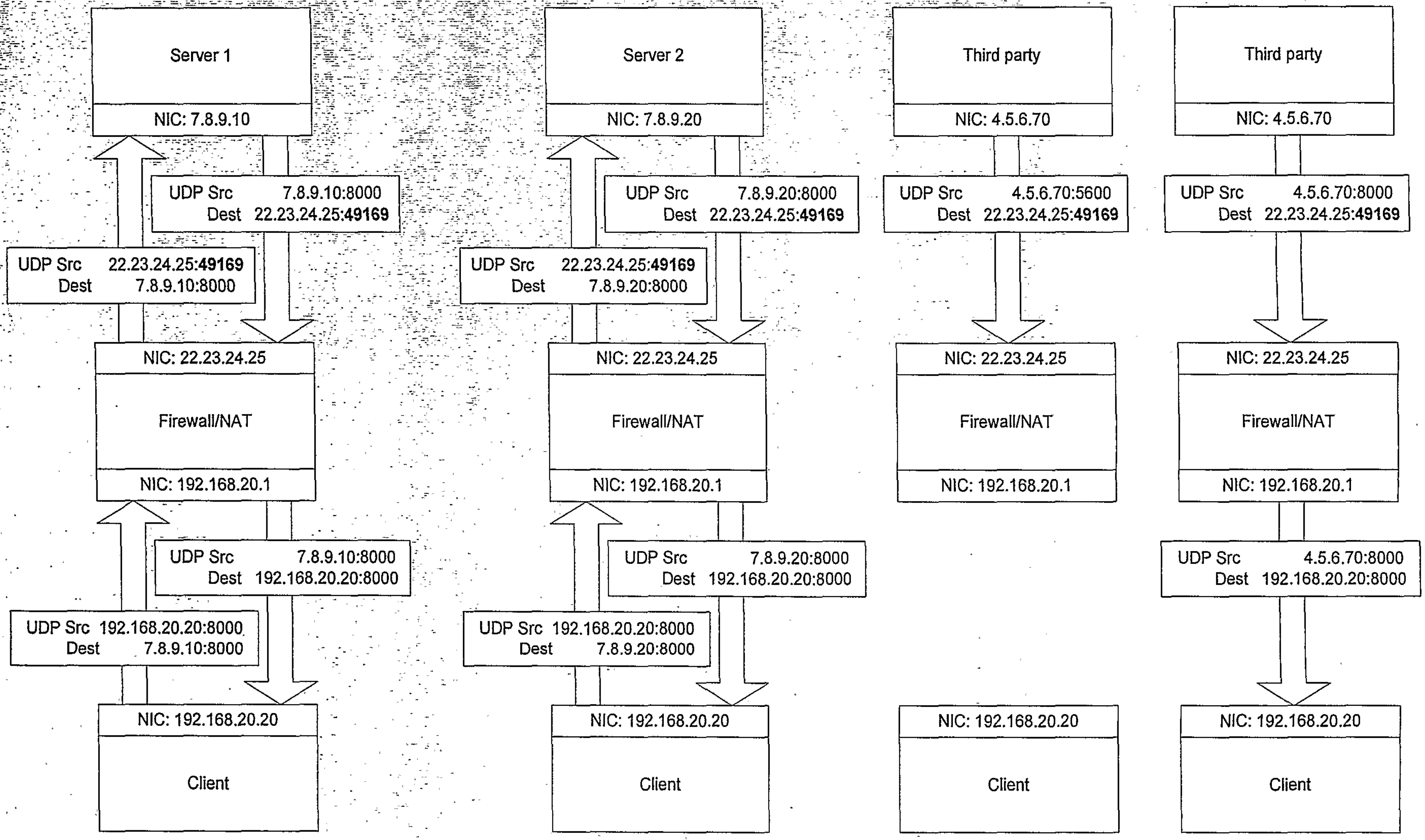
First request and response.

Second request and response.

Third party, unsolicited response with mismatched source port is not forwarded.

Third party, unsolicited response with matched source port is forwarded.

Figure 1: Client behind a Cone NAT/PAT. All requests with a given port (8000) are masqueraded. The next, and subsequent requests made to different destination addresses with that port are masqueraded to the same port. In addition, unsolicited responses from others addresses are forwarded, regardless of source port.



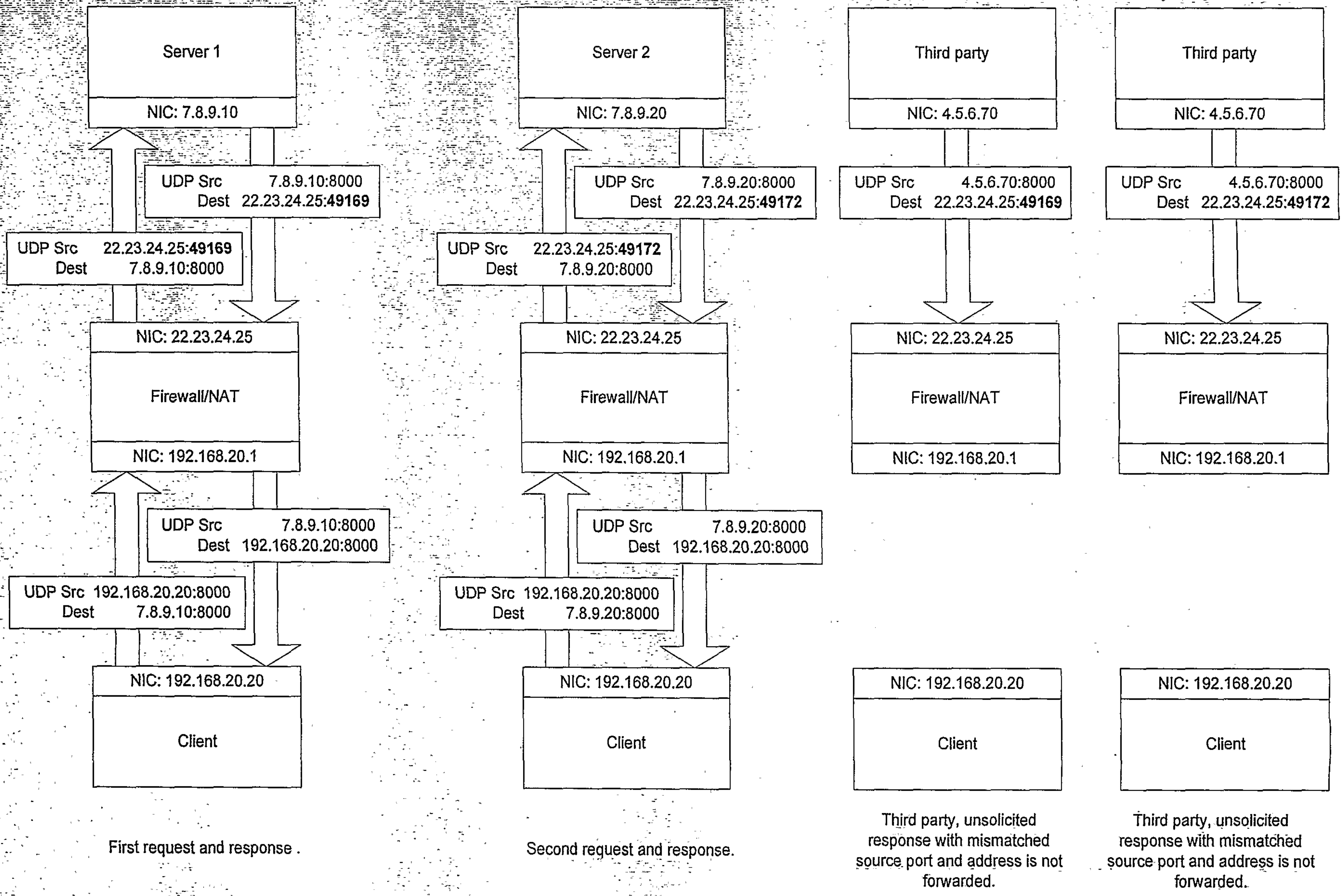
First request and response.

Second request and response.

Third party, unsolicited response with mismatched source port is not forwarded.

Third party, unsolicited response with matched source port is forwarded.

Figure 2: Client behind a Port-Restricted Cone NAT/PAT. All requests with a given port (8000) are masqueraded. The next, and subsequent requests made to different destination addresses with that port are masqueraded to the same port. In addition, unsolicited responses from others addresses are forwarded, so long as the source port matches the destination port of the original request.



First request and response .

Second request and response.

Third party, unsolicited response with mismatched source port and address is not forwarded.

Third party, unsolicited response with mismatched source port and address is not forwarded.

Figure 3: Client behind a Symmetric NAT/PAT. All requests with a given port (8000) are masqueraded. The next, and subsequent requests made to different destination addresses with that port are masqueraded to different ports. In addition, unsolicited responses from others addresses are not forwarded, because the source addresses do not match the destination of the original request., Most symmetric firewalls also require the source port to match the destination port of the original request (full tuple match).

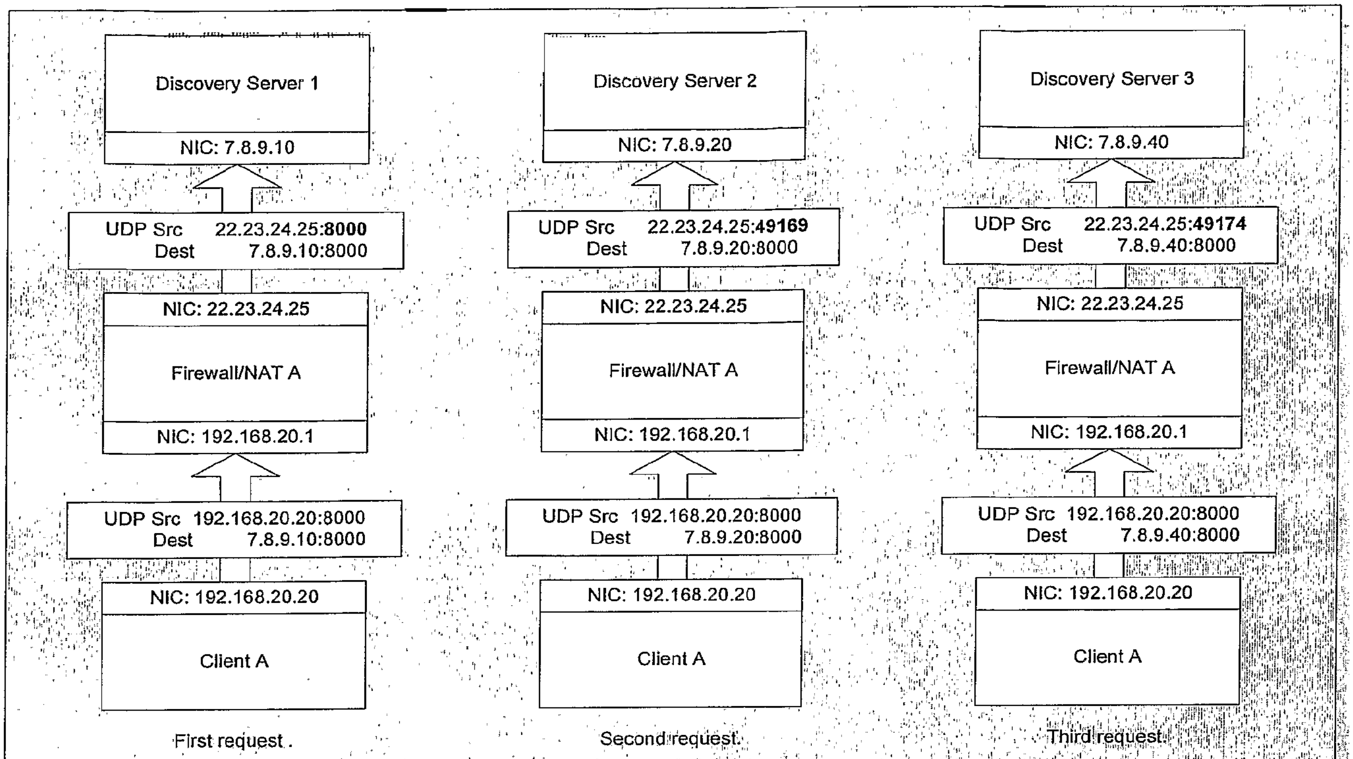


Figure 4a: Client behind a second-priority masqerading NAT/PAT. The first request with a given port (8000) is not masqueraded. The next, and subsequent requests made to different destination addresses with that port before the first one expires are masqueraded.

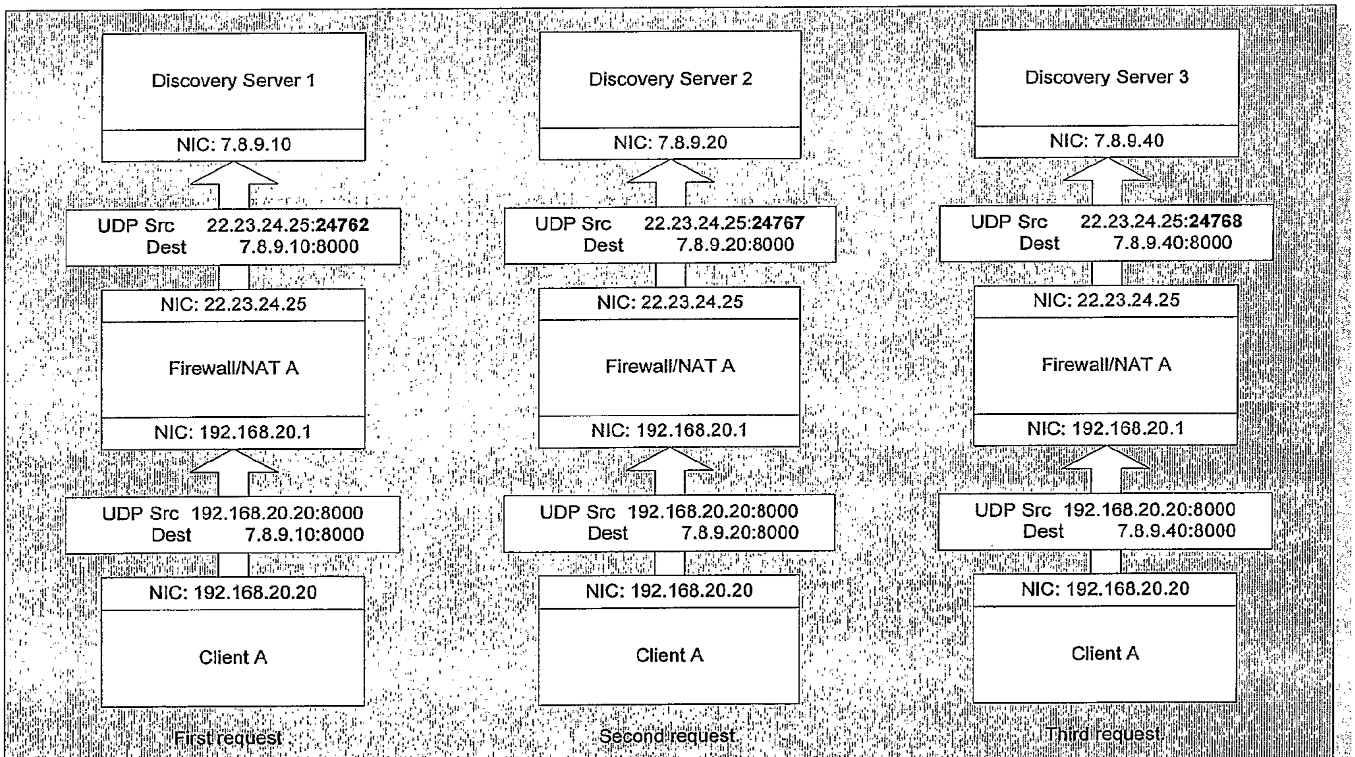


Figure 4b: Client behind a pure masqerading NAT/PAT. All requests with a given port (8000) are masqueraded. The masqueraded port changes for each destination address.

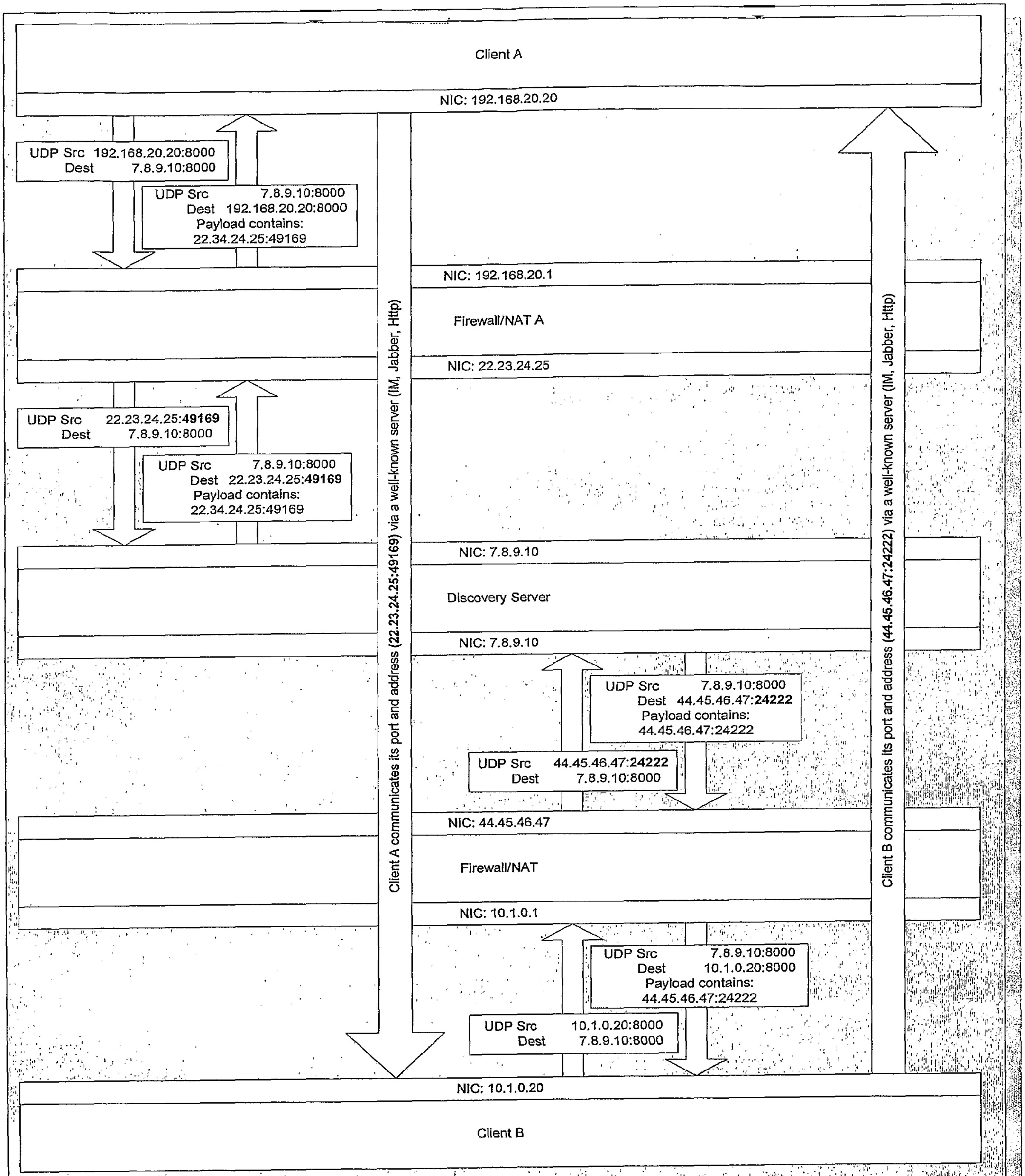


Figure 5: Connection reversal failure between clients behind symmetric NATs (left overleaf) Shows the initial discovery server requests to get masqueraded ports and external routable addresses, and the exchange of same between the clients.

FIGURE 5A

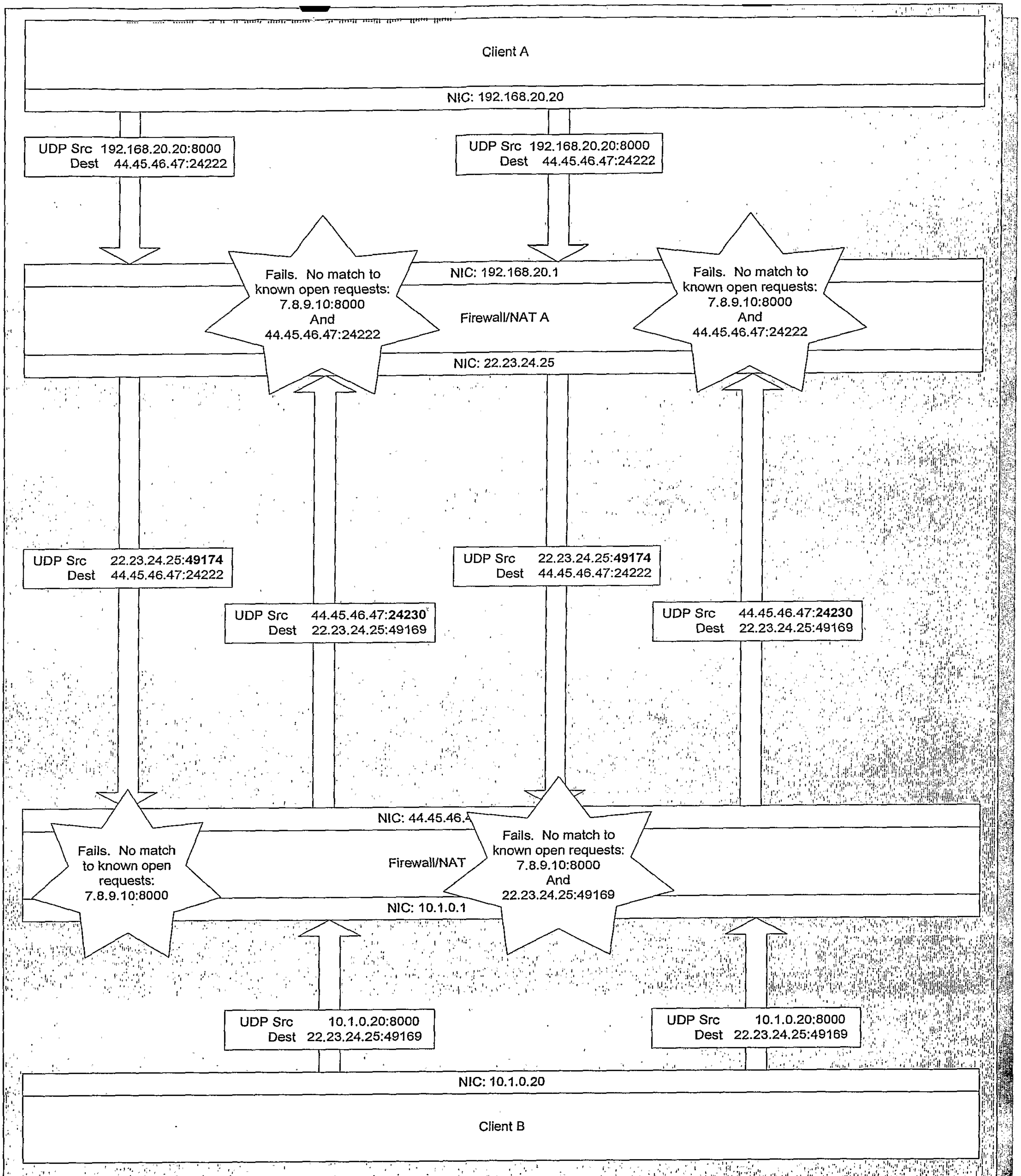
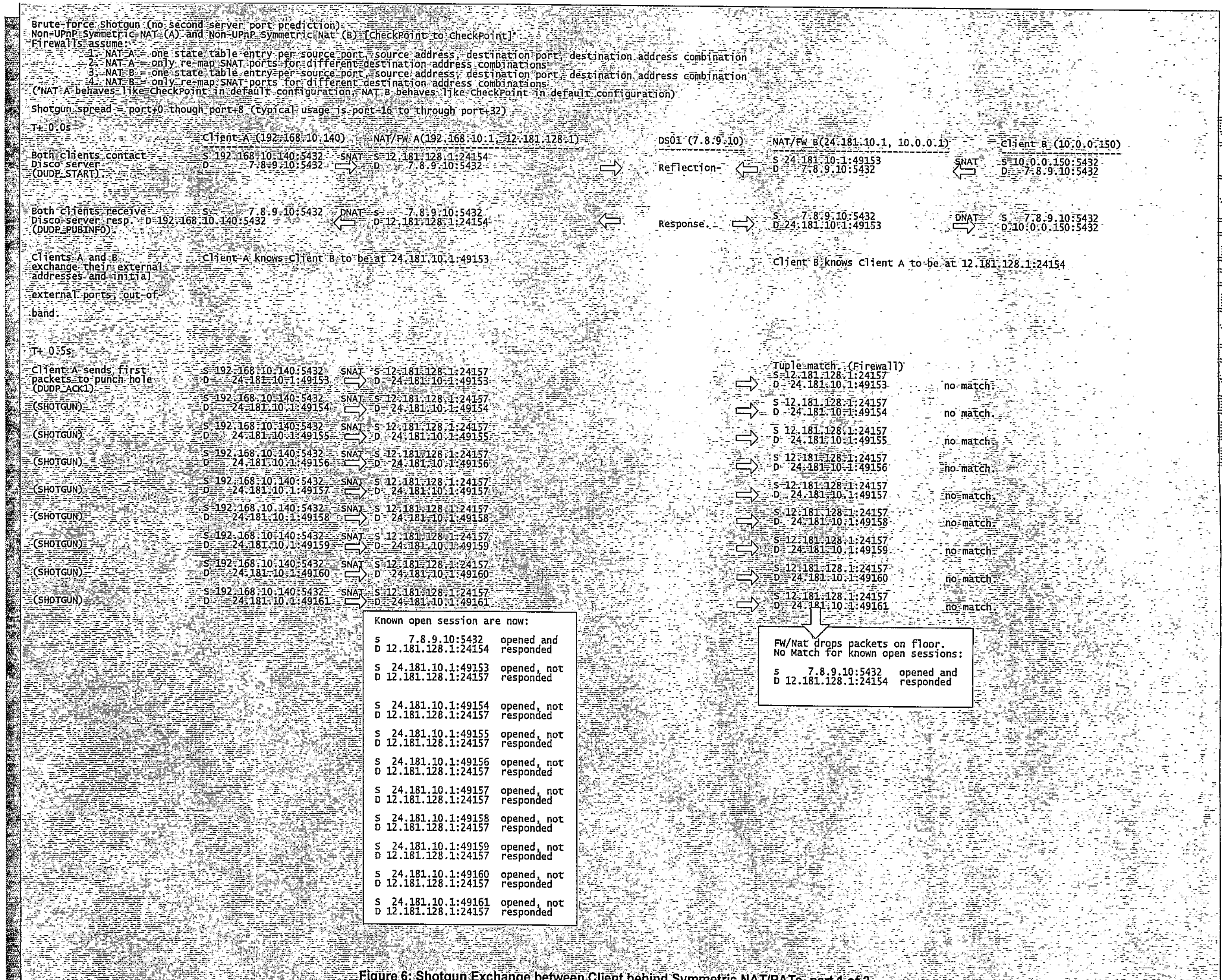

Client A
NIC: 192.168.20.20
UDP Src 192.168.20.20:8000
Dest 44.45.46.47:24222
UDP Src 192.168.20.20:8000
Dest 44.45.46.47:24222
NIC: 192.168.20.1
Fails. No match to known open requests: 7.8.9.10:8000 And 44.45.46.47:24222
Firewall/NAT A
Fails. No match to known open requests: 7.8.9.10:8000 And 44.45.46.47:24222
NIC: 22.23.24.25
UDP Src 22.23.24.25:49174
Dest 44.45.46.47:24222
UDP Src 22.23.24.25:49174
Dest 44.45.46.47:24222
UDP Src 44.45.46.47:24230
Dest 22.23.24.25:49169
UDP Src 44.45.46.47:24230
Dest 22.23.24.25:49169
NIC: 44.45.46.4
Fails. No match to known open requests: 7.8.9.10:8000
Firewall/NAT
Fails. No match to known open requests: 7.8.9.10:8000 And 22.23.24.25:49169
NIC: 10.1.0.1
UDP Src 10.1.0.20:8000
Dest 22.23.24.25:49169
UDP Src 10.1.0.20:8000
Dest 22.23.24.25:49169
NIC: 10.1.0.20
Client B

Figure 5: Connection reversal failure between clients behind symmetric NATs. (right overleaf) Shows the failed attempt to use the discovered ports to communicate directly between the clients.

FIGURE 5B



```
Brute-force Shotgun (no second server port prediction)
Non-UPnP Symmetric NAT (A) and Non-UPnP Symmetric Nat (B) [CheckPoint to CheckPoint]*
Firewalls assume:
        1. NAT A = one state table entry per source port, source address, destination port, destination address combination
        2. NAT A = only re-map SNAT ports for different destination address combinations
        3. NAT B = one state table entry per source port, source address, destination port, destination address combination
        4. NAT B = only re-map SNAT ports for different destination address combinations
(*NAT A behaves like CheckPoint in default configuration, NAT B behaves like CheckPoint in default configuration)

Shotgun spread = port+0 though port+8 (typical usage is port-16 to through port+32)

T+ 0.0s
                        Client A (192.168.10.140)      NAT/FW A(192.168.10.1, 12.181.128.1)          DS01 (7.8.9.10)    NAT/FW B(24.181.10.1, 10.0.0.1)        Client B (10.0.0.150)
Both clients contact    S 192.168.10.140:5432   SNAT   S 12.181.128.1:24154                                             S 24.181.10.1:49153          SNAT     S 10.0.0.150:5432
Disco server            D       7.8.9.10:5432   ⇨      D       7.8.9.10:5432      ⇨          Reflection-    ⇦      D     7.8.9.10:5432          ⇦       D   7.8.9.10:5432
(DUDP_START).

Both clients receive    S       7.8.9.10:5432   DNAT   S     7.8.9.10:5432                                              S     7.8.9.10:5432          DNAT     S   7.8.9.10:5432
Disco server resp.  D 192.168.10.140:5432      ⇦      D 12.181.128.1:24154       ⇦          Response.      ⇨      D 24.181.10.1:49153          ⇨       D 10.0.0.150:5432
(DUDP_PUBINFO).

Clients A and B         Client A knows Client B to be at 24.181.10.1:49153                                      Client B knows Client A to be at 12.181.128.1:24154
exchange their external
addresses and initial

external ports, out-of

band.


T+ 0.5s
                                                                                                           Tuple match. (Firewall)
Client A sends first    S 192.168.10.140:5432   SNAT   S 12.181.128.1:24157                                S 12.181.128.1:24157
packets to punch hole   D    24.181.10.1:49153  ⇨      D  24.181.10.1:49153                         ⇨      D  24.181.10.1:49153        no match.
(DUDP_ACK1)
                        S 192.168.10.140:5432   SNAT   S 12.181.128.1:24157                                S 12.181.128.1:24157
(SHOTGUN)               D    24.181.10.1:49154  ⇨      D  24.181.10.1:49154                         ⇨      D  24.181.10.1:49154        no match.
                        S 192.168.10.140:5432   SNAT   S 12.181.128.1:24157                                S 12.181.128.1:24157
(SHOTGUN)               D    24.181.10.1:49155  ⇨      D  24.181.10.1:49155                         ⇨      D  24.181.10.1:49155        no match.
                        S 192.168.10.140:5432   SNAT   S 12.181.128.1:24157                                S 12.181.128.1:24157
(SHOTGUN)               D    24.181.10.1:49156  ⇨      D  24.181.10.1:49156                         ⇨      D  24.181.10.1:49156        no match.
                        S 192.168.10.140:5432   SNAT   S 12.181.128.1:24157                                S 12.181.128.1:24157
(SHOTGUN)               D    24.181.10.1:49157  ⇨      D  24.181.10.1:49157                         ⇨      D  24.181.10.1:49157        no match.
                        S 192.168.10.140:5432   SNAT   S 12.181.128.1:24157                                S 12.181.128.1:24157
(SHOTGUN)               D    24.181.10.1:49158  ⇨      D  24.181.10.1:49158                         ⇨      D  24.181.10.1:49158        no match.
                        S 192.168.10.140:5432   SNAT   S 12.181.128.1:24157                                S 12.181.128.1:24157
(SHOTGUN)               D    24.181.10.1:49159  ⇨      D  24.181.10.1:49159                         ⇨      D  24.181.10.1:49159        no match.
                        S 192.168.10.140:5432   SNAT   S 12.181.128.1:24157                                S 12.181.128.1:24157
(SHOTGUN)               D    24.181.10.1:49160  ⇨      D  24.181.10.1:49160                         ⇨      D  24.181.10.1:49160        no match.
                        S 192.168.10.140:5432   SNAT   S 12.181.128.1:24157                                S 12.181.128.1:24157
(SHOTGUN)               D    24.181.10.1:49161  ⇨      D  24.181.10.1:49161                         ⇨      D  24.181.10.1:49161        no match.

                                               Known open session are now:                                 FW/Nat drops packets on floor.
                                                                                                           No Match for known open sessions:
                                               S      7.8.9.10:5432   opened and
                                               D 12.181.128.1:24154   responded                            S      7.8.9.10:5432   opened and
                                                                                                           D 12.181.128.1:24154   responded
                                               S  24.181.10.1:49153   opened, not
                                               D 12.181.128.1:24157   responded


                                               S  24.181.10.1:49154   opened, not
                                               D 12.181.128.1:24157   responded

                                               S  24.181.10.1:49155   opened, not
                                               D 12.181.128.1:24157   responded

                                               S  24.181.10.1:49156   opened, not
                                               D 12.181.128.1:24157   responded

                                               S  24.181.10.1:49157   opened, not
                                               D 12.181.128.1:24157   responded

                                               S  24.181.10.1:49158   opened, not
                                               D 12.181.128.1:24157   responded

                                               S  24.181.10.1:49159   opened, not
                                               D 12.181.128.1:24157   responded

                                               S  24.181.10.1:49160   opened, not
                                               D 12.181.128.1:24157   responded

                                               S  24.181.10.1:49161   opened, not
                                               D 12.181.128.1:24157   responded
```

Figure 6: Shotgun Exchange between Client behind Symmetric NAT/PATs, part 1 of 2.

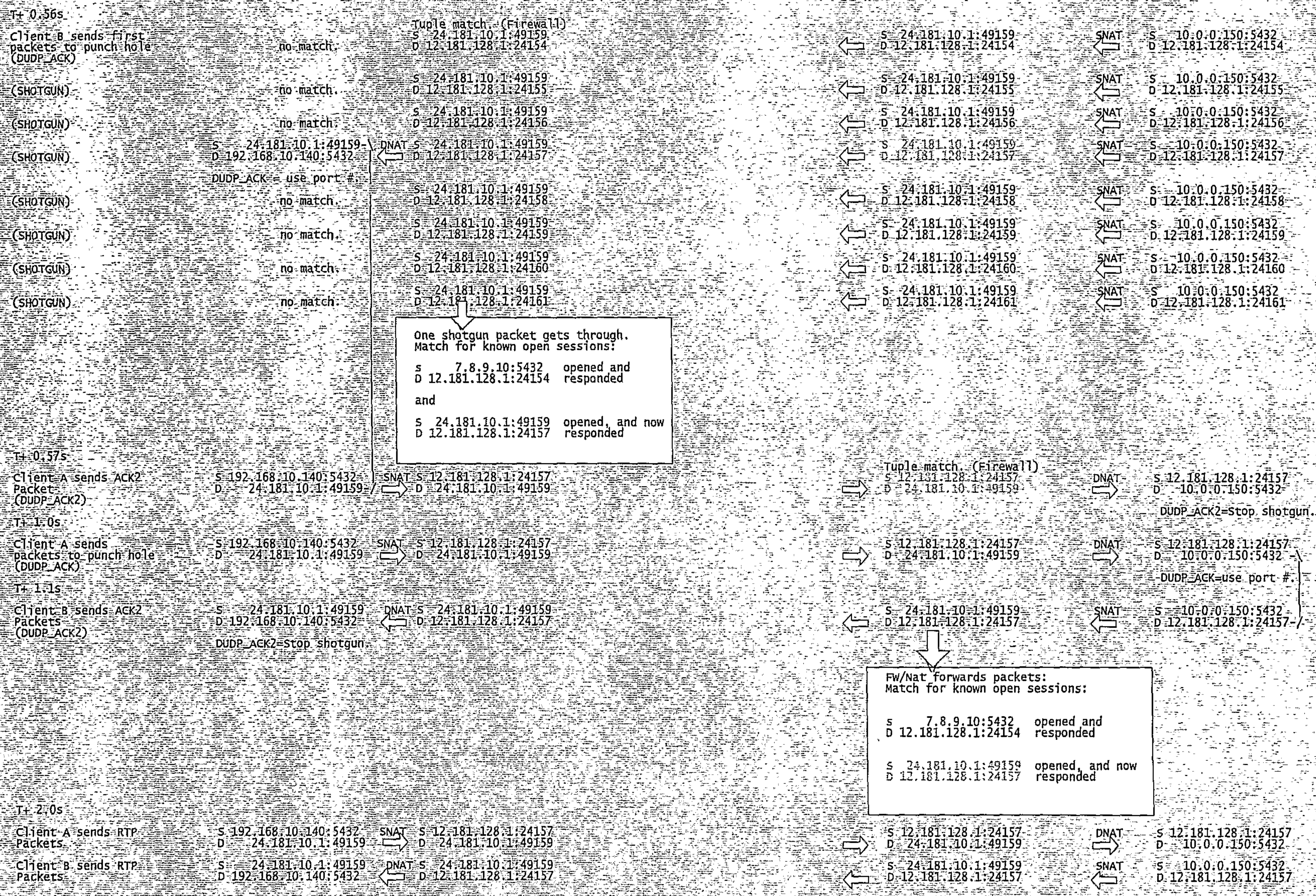


Figure 6: Shotgun Exchange between Client behind Symmetric NAT/PATs, part 2 of 2.

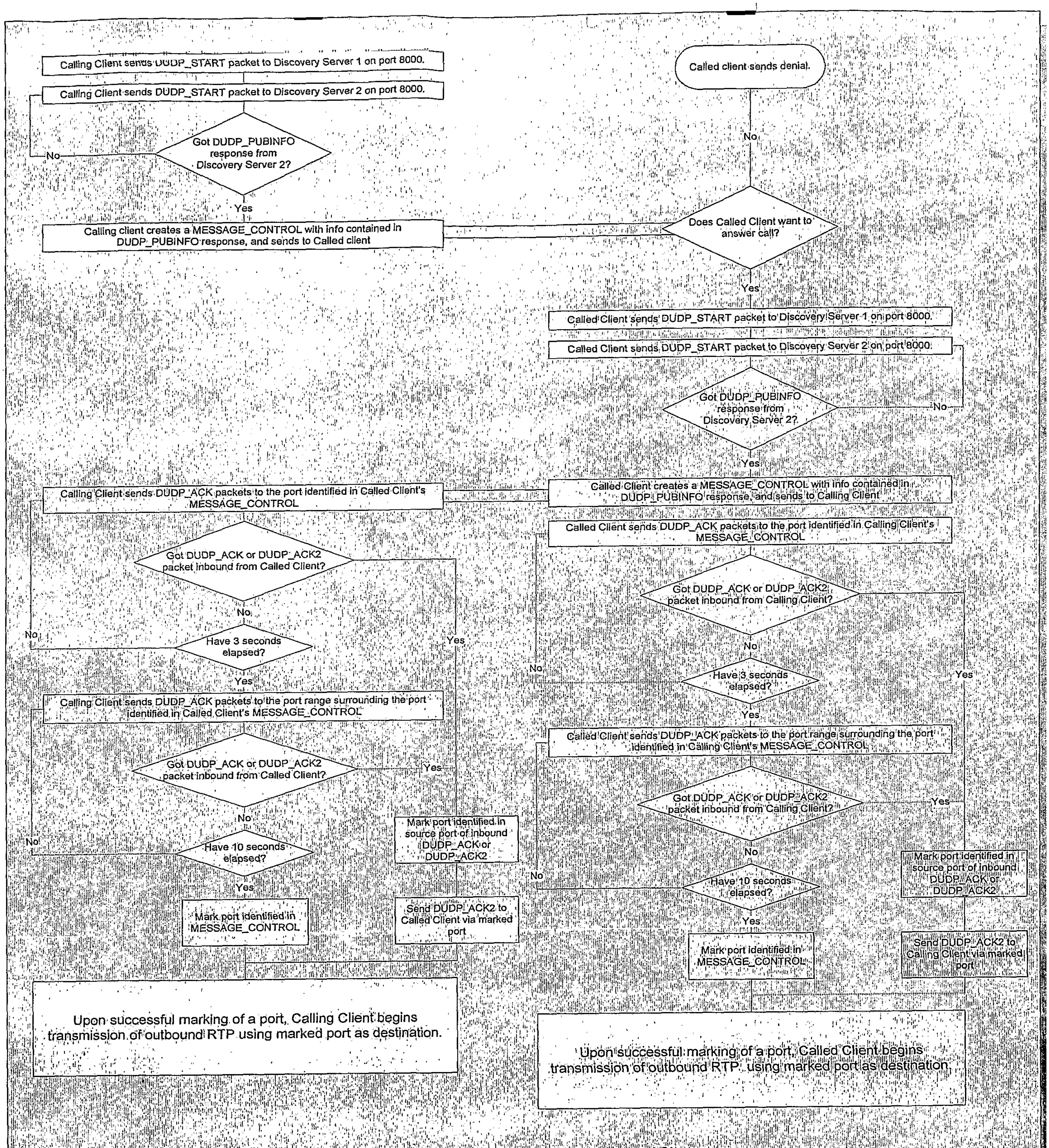

Calling Client sends DUDP_START packet to Discovery Server 1 on port 8000.
Calling Client sends DUDP_START packet to Discovery Server 2 on port 8000.
Got DUDP_PUBINFO response from Discovery Server 2?
No
Yes
Calling client creates a MESSAGE_CONTROL with info contained in DUDP_PUBINFO response, and sends to Called client
Called client sends denial.
No
Does Called Client want to answer call?
Yes
Called Client sends DUDP_START packet to Discovery Server 1 on port 8000.
Called Client sends DUDP_START packet to Discovery Server 2 on port 8000.
Got DUDP_PUBINFO response from Discovery Server 2?
No
Yes
Called Client creates a MESSAGE_CONTROL with info contained in DUDP_PUBINFO response, and sends to Calling Client
Calling Client sends DUDP_ACK packets to the port identified in Called Client's MESSAGE_CONTROL
Got DUDP_ACK or DUDP_ACK2 packet inbound from Called Client?
No
Yes
Have 3 seconds elapsed?
No
Yes
Calling Client sends DUDP_ACK packets to the port range surrounding the port identified in Called Client's MESSAGE_CONTROL
Got DUDP_ACK or DUDP_ACK2 packet inbound from Called Client?
Yes
No
Have 10 seconds elapsed?
No
Yes
Mark port identified in MESSAGE_CONTROL
Mark port identified in source port of inbound DUDP_ACK or DUDP_ACK2
Send DUDP_ACK2 to Called Client via marked port
Upon successful marking of a port, Calling Client begins transmission of outbound RTP using marked port as destination.
Called Client sends DUDP_ACK packets to the port identified in Calling Client's MESSAGE_CONTROL
Got DUDP_ACK or DUDP_ACK2 packet inbound from Calling Client?
No
Yes
Have 3 seconds elapsed?
No
Yes
Called Client sends DUDP_ACK packets to the port range surrounding the port identified in Calling Client's MESSAGE_CONTROL
Got DUDP_ACK or DUDP_ACK2 packet inbound from Calling Client?
Yes
No
Have 10 seconds elapsed?
No
Yes
Mark port identified in MESSAGE_CONTROL
Mark port identified in source port of inbound DUDP_ACK or DUDP_ACK2
Send DUDP_ACK2 to Calling Client via marked port
Upon successful marking of a port, Called Client begins transmission of outbound RTP using marked port as destination.

Figure 7: Flowchart of Discovery, Message Exchange, and Shotgun process

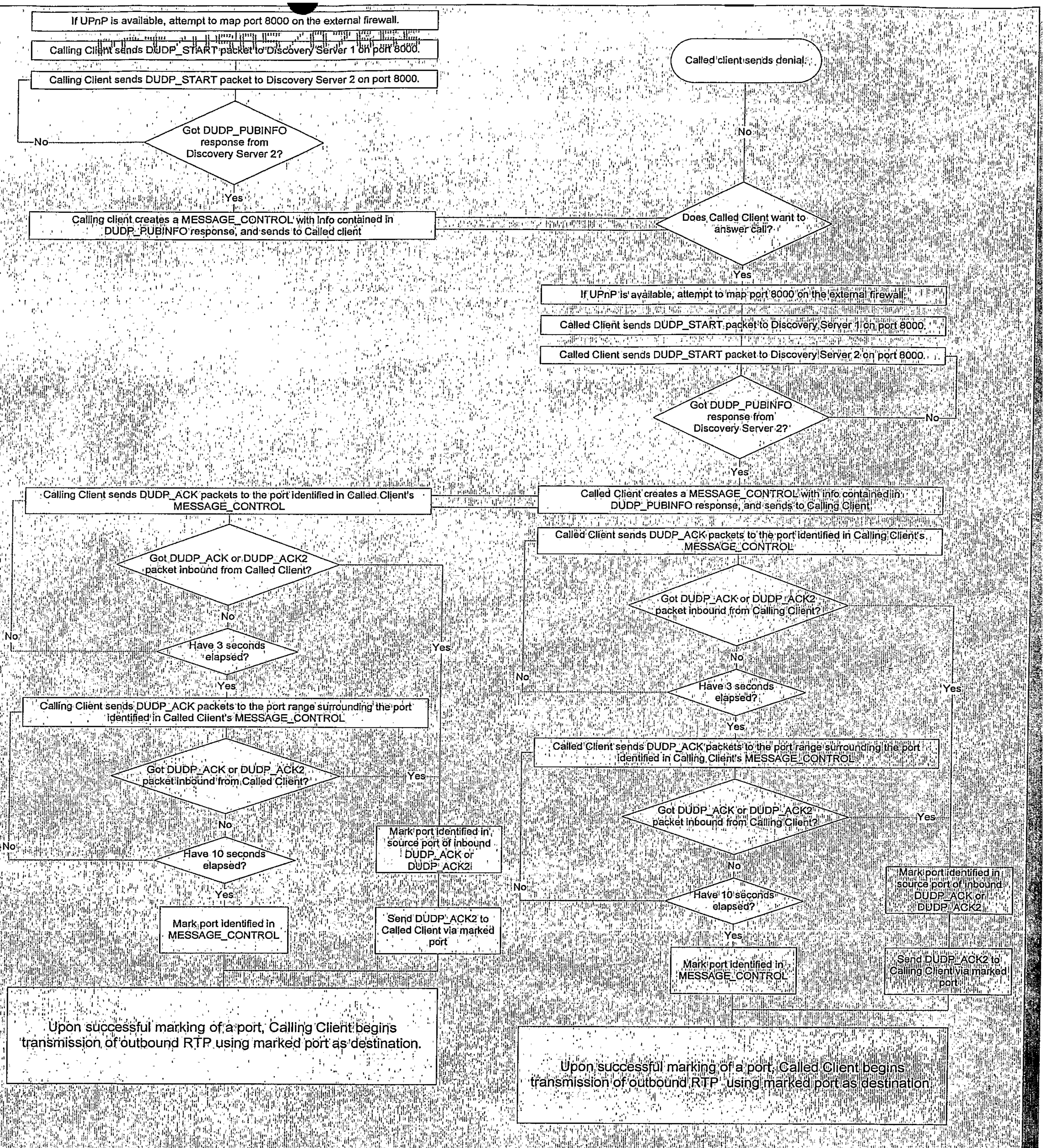

If UPnP is available, attempt to map port 8000 on the external firewall.
Calling Client sends DUDP_START packet to Discovery Server 1 on port 8000.
Calling Client sends DUDP_START packet to Discovery Server 2 on port 8000.
Got DUDP_PUBINFO response from Discovery Server 2?
No
Yes
Calling client creates a MESSAGE_CONTROL with info contained in DUDP_PUBINFO response, and sends to Called client
Called client sends denial.
No
Does Called Client want to answer call?
Yes
If UPnP is available, attempt to map port 8000 on the external firewall.
Called Client sends DUDP_START packet to Discovery Server 1 on port 8000.
Called Client sends DUDP_START packet to Discovery Server 2 on port 8000.
Got DUDP_PUBINFO response from Discovery Server 2?
No
Yes
Called Client creates a MESSAGE_CONTROL with info contained in DUDP_PUBINFO response, and sends to Calling Client
Calling Client sends DUDP_ACK packets to the port identified in Called Client's MESSAGE_CONTROL
Got DUDP_ACK or DUDP_ACK2 packet inbound from Called Client?
No
Yes
No
Have 3 seconds elapsed?
Yes
Calling Client sends DUDP_ACK packets to the port range surrounding the port identified in Called Client's MESSAGE_CONTROL
Got DUDP_ACK or DUDP_ACK2 packet inbound from Called Client?
Yes
No
No
Have 10 seconds elapsed?
Yes
Mark port identified in source port of inbound DUDP_ACK or DUDP_ACK2
Mark port identified in MESSAGE_CONTROL
Send DUDP_ACK2 to Called Client via marked port
Upon successful marking of a port, Calling Client begins transmission of outbound RTP using marked port as destination.
Called Client sends DUDP_ACK packets to the port identified in Calling Client's MESSAGE_CONTROL
Got DUDP_ACK or DUDP_ACK2 packet inbound from Calling Client?
No
No
Yes
Have 3 seconds elapsed?
Yes
Called Client sends DUDP_ACK packets to the port range surrounding the port identified in Calling Client's MESSAGE_CONTROL
Got DUDP_ACK or DUDP_ACK2 packet inbound from Calling Client?
Yes
No
No
Have 10 seconds elapsed?
Yes
Mark port identified in source port of inbound DUDP_ACK or DUDP_ACK2
Mark port identified in MESSAGE_CONTROL
Send DUDP_ACK2 to Calling Client via marked port
Upon successful marking of a port, Called Client begins transmission of outbound RTP using marked port as destination.

Figure 8: Flowchart of Discovery, Message Exchange, and Shotgun process, including UPnP

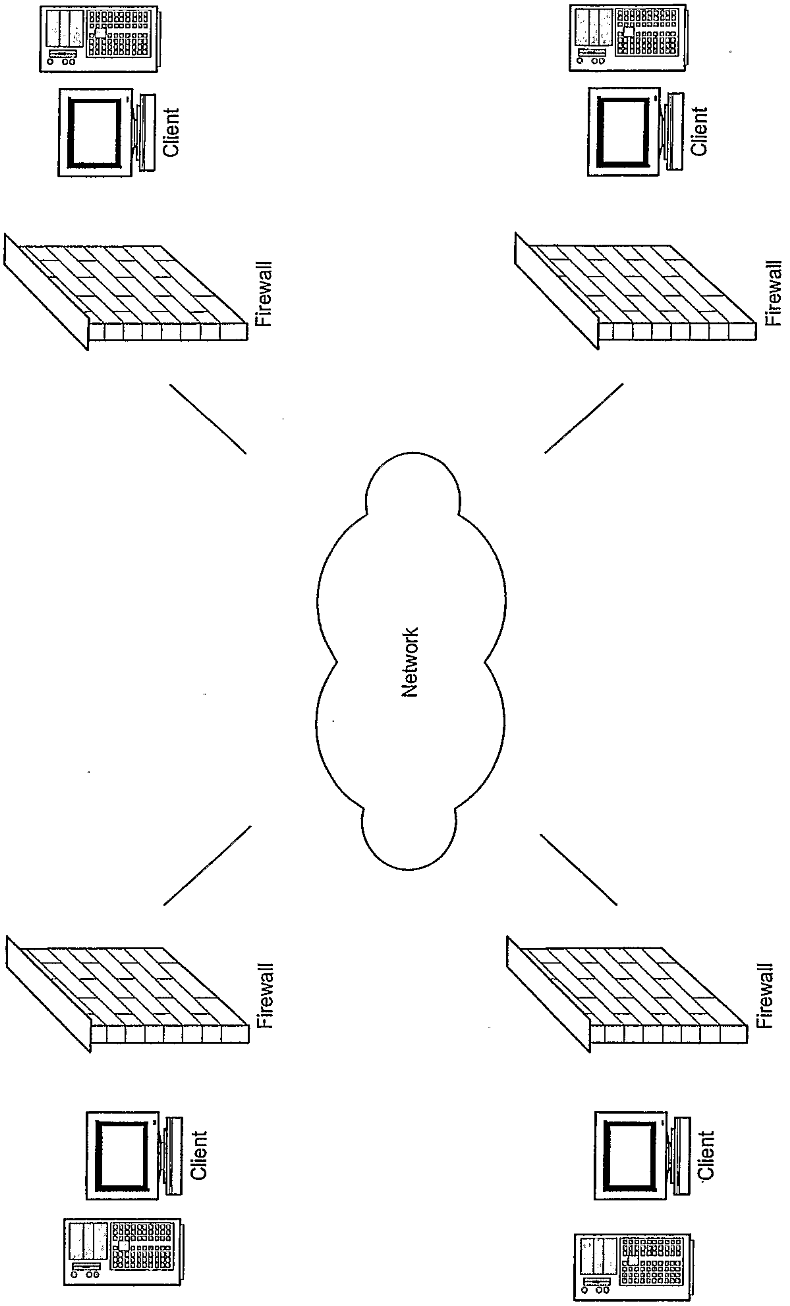

Client
Firewall
Client
Firewall
Network
Firewall
Client
Firewall
Client

FIGURE 9